Re: Overview of Patient Consent Models (Opt-in/Opt-out)

I. Introduction

This paper presents a general overview of the approaches currently in use with respect to the granting to patients of a choice whether their electronic personal health information can be transferred to third parties by means of a health information exchange (HIE). It was prepared under the auspices of the State of Illinois Office of Health Information Technology for the use of the Illinois Health Information Exchange Authority Data Security and Privacy Committee.[1]

II. Current Illinois Law and Practice on Privacy, Security, and Consent

Development and implementation of the state-level Illinois Health Information Exchange (ILHIE) are affected by both Federal and State laws, many of which impose disclosure restrictions on certain custodians of health data (e.g., "covered entities" and "business associates")[2]. In addition, many Federal and State laws require advance patient consent to exchange health data in certain circumstances. Such laws can affect the operation and architecture of the HIE, including what type of health data can be sent to or retrieved from the HIE, what type of providers can participate in the HIE, and for what purpose health data can be exchanged.

A. General Privacy

In addition to Federal protections, Illinois has State-level laws in place to protect patient privacy. The Illinois Medical Patient Rights Act (1989),[3] which predates HIPAA regulations, provides that a custodian of health information (or data) shall "refrain from disclosing the nature or details of services provided to patients" without patient authorization. The Medical Patient Rights Act contains certain exceptions to this restriction, which are conceptually similar to,

[1] The General Counsel of OHIT gratefully acknowledges the assistance of Sarah Nelson, OHIT Legal Intern, as this paper's primary author, and the legal research assistance of the following OHIT Legal Interns: Abraham Arnold; Daniel Pomierski; April Kusper Schweitzer; Sarah Sullivan; and Melissa Tyler.

[2] The Federal Health Insurance Portability and Accountability Act (HIPAA) imposes various privacy and security obligations upon "covered entities", generally health care providers, payers and clearinghouses, and upon "business associates", generally agents of "covered entities", with respect to their treatment of "PHI", generally personally-identifiable patient health data. Under current proposed HIPAA rules, HIEs are generally deemed to be "business associates".

[3] 410 ILCS 50/0.01 et seq.; see also Hospital Licensing Act, 210 ILCS 85/6.17d.

though more limited than, HIPAA's T-P-O exceptions[4]. For example, the Medical Patient Rights Act does not expressly recognize the existence and role of "business associates" and their non-medical ancillary/agency role in the delivery of healthcare. Whereas HIPAA provides an express basis for invoking a T-P-O and "business associate" exception to justify the disclosure of non-specifically-protected PHI without prior patient authorization to an HIE, the availability of a similar exception under current Illinois law is less clear.

B. Specially Protected Health Information (PHI)

Illinois, like many other States, has enacted laws that provide heightened privacy protection for certain types of health data. By statute, Illinois imposes specific patient consent requirements with respect to the disclosure of health data involving mental health and developmental disability services, genetic information testing, testing for and treatment of HIV/AIDs/sexually-transmissible diseases, treatment of alcoholism and drug abuse, treatment of child neglect and abuse, and treatment of sexual assault and abuse.[5] Illinois statute imposes higher privacy standards than those imposed by HIPAA regulations. Thus, Illinois statutory consent requirements must be followed even when the disclosure of information would otherwise be permitted under HIPAA regulations without patient consent or authorization.

C. Security Standards

In general, Illinois law does not impose security standards in excess of Federal standards. Under the HIPAA Security Rule,[6] a "covered entity" or "business associate" must comply with specific security standards regarding the confidentiality, integrity, and availability of stored PHI data, precautionary measures regarding reasonably anticipated threats and misuse, and workforce compliance measures. In addition to the security standards, specific rules address administrative safeguards, physical safeguards, technical safeguards, organizational requirements, policies, and procedures, and documentation requirements. The comprehensive Federal standards include security "breach notification" response and reporting obligations.

[4] HIPAA, 45 CFR§164.506. The Federal HIPAA Privacy Rule requires patient authorization/consent for all PHI disclosures unless expressly permitted. A specific exception exists for certain disclosures for purposes of "Treatment, Payment and Healthcare Operations" (a/k/a T-P-O).

[5] e.g., Alcoholism and Other Drug Abuse and Dependency Act, 20 ILCS 301/30-5; AIDS Confidentiality Act, 410 ILCS 305/; Genetic Information Privacy Act, 410 ILCS 513/; Illinois Sexually Transmissible Disease Control Act, 410 ILCS 325/; Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/.

[6] 45 C.F.R. § 164.306-16.

III. Consent Models

The issues of whether, to what extent, and how individuals should have control over their personal health information are among the foremost policy challenges related to the electronic exchange of health data.[7] States implementing HIEs must balance the diverse and sometimes contrasting interests of multiple key stakeholders, including patients, providers, provider organizations, payer organizations, and others. Maximizing patient and provider participation, in particular, is a key goal in terms of enhancing the quality and delivery of patient-centered healthcare and promoting public health.

Five core consent models for health data have been identified, with the models differing in the level or extent of patient choice or input.[8] The models fall into three broad categories and have contrasting advantages and disadvantages from the perspectives of key stakeholders. All of the models operate within the bounds established by applicable Federal and State laws, including for the exchange of sensitive health data. Thus, patient consent in the respective models can be viewed as the consent required (or provided) above the baseline established by Federal and State laws. In addition, the models apply specifically to participation in networked electronic exchanges (HIEs) and are not intended to constrain the transmission of health data for the purposes of treatment, payment, and healthcare operations (T-P-O) as permitted under HIPAA and other relevant Federal and State laws.[9]

A. The Five Core Consent Models for Health Data

A Model Involving No Consent

> 1. **No-consent Model**: The default is for all health data (or some pre-defined set of health data as determined by the HIE) to be eligible automatically for electronic exchange, with no provision or opportunity for patient consent.[10]

This model does not allow for patient preference with respect to participation in the HIE, with the health data of all patients being automatically included in the HIE. Thus, electronic exchange

[7] Melissa M. Goldstein and Alison L. Rein, *Consumer Consent Options for Electronic Health Information Exchange: Policy Considerations and Analysis*, pp. 93 (2010a); Melissa M. Goldstein and Alison L. Rein, *Data Segmentation in Electronic Health Information Exchange: Policy Considerations and Analysis*, pp. 74 (2010b);
[8] Goldstein and Rein 2010a at 5-7.
[9] Goldstein and Rein 2010a at 5.
[10] Goldstein and Rein 2010a at 5.

can take place without obtaining patient consent and irrespective of patient preference for participation in the HIE. One permutation of this model involves the inclusion of a minimal requirement that patients be notified of their participation in the HIE and educated as to what the HIE does and what purposes are served by electronic exchange of health data in terms of the quality and delivery of patient-centered care.[11]

Consent Models Involving Opt-out or Opt-in In Full

> 2. **Opt-out In Full Model**: The default is for all health data (or some pre-defined set of health data as determined by the HIE) to be eligible automatically for electronic exchange, but with a provision that each patient must be given the opportunity to opt-out in full.[12]
>
> 3. **Opt-in In Full Model**: The default is for no health data to be eligible automatically for electronic exchange. Patients wishing to make all health data (or some pre-defined set of health data as determined by the HIE) eligible for electronic exchange must actively express their desire to participate (i.e., affirmatively opt-in in full).[13]

Both models allow for patient preference (or consent) with respect to participation in the HIE, yet neither provides the opportunity for granularity (see below) in that preference. In other words, patients wishing to opt-out or opt-in can only do so in full. For the Opt-out model, there are at least two scenarios: either the health data of the patient who opts out are collected through the HIE but are never shared with other providers (being used only for legally permitted purposes such as public health reporting) or the health data never enter the HIE in the first place (i.e., the opt-out preference is recorded prior to data entry).[14]

Consent Models Involving Opt-out or Opt-in With Granularity

> 4. **Opt-out With Exceptions Model**: The default is for all health data (or some pre-defined set of health data as determined by the HIE) to be eligible automatically for electronic exchange, but with a provision that each patient must be given the opportunity either to opt-out in full (as above) or to (1) exclude specific categories or elements of health data from the exchange, (2) limit the

[11] Goldstein and Rein 2010a at 6.
[12] Goldstein and Rein 2010a at 6.
[13] Goldstein and Rein 2010a at 7.
[14] Goldstein and Rein 2010a at 6.

> exchange of health data to specific providers or provider organizations, or (3) limit the exchange of health data for specific purposes.[15]
>
> 5. **Opt-in With Restrictions Model**: The default is for no health data to be eligible automatically for electronic exchange. Patients wishing to make all health data (or some pre-defined set of health data as determined by the HIE) eligible for electronic exchange must actively express their desire to participate (i.e., affirmatively opt-in). Patients must be given the opportunity either to opt-in in full (as above) or to (1) include only specific elements or categories of health data in the exchange, (2) allow the flow of health data only to specific providers or provider organizations, or (3) allow the exchange of health data only for specific purposes.[16]

Both models allow for patient preference (or consent) with respect to participation in the HIE. In addition, the granularity options in the two models enable patients who choose to participate in the HIE to exert some control over the type of health data that can be shared, to restrict the data accessed via the HIE to a limited set of providers (or provider organizations), or to specify the purposes (broadly or narrowly) for which the health data are exchanged.

B. Granularity and Data Segmentation

The granularity options in Models 4 and 5 above fall into three broad categories: data type, provider, and purpose.[17]

Granularity by data type enables patients to block the electronic exchange of specific health data elements (e.g., a recent laboratory test) or categories of health data (e.g., all medications). Such a granularity option tends to be viewed more favorably by patients and consumer advocates than by providers and those responsible for implementing the HIEs. For patients, the option provides them with more selective control over the exchange of their personal health data. For providers, the option potentially limits their access to full and complete health data about patients, which in turn may significantly constrain their ability to provide the highest quality and most effective care. For those responsible for implementing the HIEs, the option may significantly increase the technological, logistical, and administrative challenges of tracking and implementing the varied choices for each patient in the HIE. Yet, granularity by data type already exists at some level in HIEs because of Federal and State laws governing the

[15] Goldstein and Rein 2010a at 6.
[16] Goldstein and Rein 2010a at 7.
[17] Goldstein and Rein 2010a at 7-12.

exchange and flow of sensitive health data.[18] In Illinois, for example, such sensitive health data include mental health and developmental disability services, genetic information testing, testing for and treatment of HIV/AIDs/sexually-transmissible diseases, treatment of alcoholism and drug abuse, treatment of child neglect and abuse, and treatment of sexual assault and abuse.[19]

Granularity by provider restricts the flow or exchange of health data in the HIE only to those providers approved by the patient. Patients are given the option of restricting the flow only to specific individual providers, to specific provider types (e.g., to MDs only, not to supporting staff), or to specific provider entity levels (e.g., cardiologist practices but not allergist practices). As with granularity by data type, granularity by provider tends to be viewed more favorably by patients and consumer advocates than by providers and by the individuals responsible for implementing and managing the HIEs. For providers, in particular, this granularity option may constrain the efficient and effective coordination of care for individual patients among physicians and facilities.

Granularity by purpose involves segmentation according to the intended use (or purpose) for which health data can be accessed in the HIE.[20] Patients are given the option of considering all possible uses of health data in an HIE (e.g., treatment, clinical research, health services research, etc.), then allowed to block certain uses (except for those allowed by Federal or State laws, such as public health reporting and surveillance).[21] For patients, this granularity option allows for some control of the exchange of health data and may enable them to approve uses of particular interest to them (e.g., clinical or epidemiological research on heritable diseases). Assuming that most or all patients would view treatment as an approved use, this granularity option is more highly preferred by providers than the previous two options in that it allows for access to complete health data for treatment purposes and thus facilitates effective and highly coordinated care.[22] Yet challenges with this granularity option may arise in a manner similar to those surrounding implementation of the T-P-O exceptions for PHI in the HIPAA regulations. Though the treatment (T) and payment (P) elements are straightforward and generally supported by patients and providers, the healthcare operations (O) element is very

[18] Goldstein and Rein 2010a at 9.
[19] e.g., Alcoholism and Other Drug Abuse and Dependency Act, 20 ILCS 301/30-5; AIDS Confidentiality Act, 410 ILCS 305/; Genetic Information Privacy Act, 410 ILCS 513/; Illinois Sexually Transmissible Disease Control Act, 410 ILCS 325/; Mental Health and Developmental Disabilities Confidentiality Act, 740 ILCS 110/.
[20] Goldstein and Rein 2010a at 10.
[21] Goldstein and Rein 2010a at 10.
[22] Goldstein and Rein 2010a at 11.

open-ended and has proven to be more challenging for various stakeholders to interpret and implement, especially in a rapidly changing healthcare landscape.[23]

Other vectors of data sequestration -- in addition to these major granularity options, there are other possible options, such as granularity by time range.[24] As with granularity by data type, provider, or purpose, these additional options offer a mix of advantages and disadvantages for different HIE stakeholders.

The various granularity options are designed to provide patients with a range of choices, and thus are based on the view that enabling the expression of patient preference with respect to electronic sharing of health data is important in promoting patient engagement in HIEs.[25] The granularity options reflect the underlying principle (or concept) of data segmentation, which is defined as the sequestering from capture, access, or view certain data elements that are perceived by an individual (or other entity) as being undesirable to share.[26] Segmentation of sensitive health data is a prime example, with Federal or State laws imposing limits on its exchange and flow, as discussed previously.

C. Stakeholder Perspectives and the Advantages/Disadvantages of the Consent Models

As highlighted above, perspectives on the different consent models and associated options can vary depending on the interests and needs of the major stakeholders in the HIE, including patients, providers, provider organizations, payer organizations, and the individuals responsible for implementing and managing the HIEs. Key to the success of an HIE is finding and maintaining the proper balance among the interests of those diverse stakeholders.[27]

Patients

[23] Goldstein and Rein 2010a at 11-12.
[24] Goldstein and Rein 2010a at 10.
[25] Goldstein and Rein 2010b at ES-III.
[26] Goldstein and Rein 2010b at 2.
[27] Goldstein and Rein 2010a at 24-28.

Re: Overview of Patient Consent Models (Opt-in/Opt-out)

The results of patient surveys and focus groups, including the Markle Foundation survey of public attitudes about electronic exchange of personal health information[28], suggest that patients generally want providers to have access to the best and most complete data available to enable the delivery of high quality care.[29] Patients also generally recognize the value of electronic exchange of health data for improving care coordination, reducing the number of repeated and unnecessary tests and procedures, and reducing required paperwork. Yet, many patients, especially those with major privacy concerns, have indicated that being able to maintain control over electronic access to specific health data (or categories of health data) would likely increase their trust and willingness to participate in HIEs. Whereas the Opt-out in Full and Opt-in In Full Models enable patients to choose whether or not to participate in an HIE, both models enforce an all-or-nothing decision. By contrast, models involving opt-out or opt-in with granularity provide for more refined decision-making and control.[30] This is especially true for the Opt-in With Restrictions Model, which appears to provide patients with the greatest level of control. Yet such a model places a significant responsibility on patients to fully understand the meaning and implications of the various restrictions (as well as of the initial opt-in itself), plus a significant burden on providers and HIEs in terms of educating patients and the broader public about those implications.

Providers

Providers participating in HIEs value comprehensive and consistent access to health data, which enhances their ability to deliver high quality and well-coordinated patient-centered care.[31]

[28] Markle Foundation, *Survey Finds Americans Want Electronic Personal Health Information to Improve Own Health Care* (2006). Available at http://www.markle.org/publications/1214-survey-finds-americans-want-electronic-personal-health-information-improve-own-hea
[29] Goldstein and Rein 2010a at 24.
[30] Goldstein and Rein 2010a at 25.
[31] Goldstein and Rein 2010a at 25.

They also seek assurance that their reliance on HIEs for health data will not increase liability exposure and will not substantially increase administrative, technical, and financial burdens in terms of obtaining and managing patient consent. As a result, providers generally prefer consent models that maximize both the number of patients participating in an HIE and the amount of health data available through the HIE for each patient. Whereas an Opt-in with Restrictions Model may be the most highly favored by many patients, such a model may be the least favored by many providers specifically because it risks constraining the amount of health data available for patients choosing to participate in an HIE and likely lowers the total number of participating patients.

Provider Organizations

Provider organizations share the same concerns as individual providers with respect to the administrative, technical, and financial burdens associated with obtaining and managing patient consent.[32] For provider organizations, the concerns are greatly amplified because of the need to obtain and manage consent across the large set (or population) of enrolled patients. The experiences of provider organizations with HIPAA regulations demonstrated that initial costs for training staff, implementing new patient consent procedures, and modifying workflow processes to ensure compliance increased with organizational size.[33] The abilities of provider organizations, especially larger ones, to more effectively serve culturally and medically diverse populations, to facilitate research and other partnerships, and to benefit financially likely are enhanced by consent models that generate the highest level of patient participation in the HIE and provide for the most accurate and complete patient records.[34] Thus, provider organizations

[32] Goldstein and Rein 2010a at 26.
[33] Goldstein and Rein 2010a at 26.
[34] Goldstein and Rein 2010a at 27.

may have reasons to prefer "low-resistance" consent models[35], such as the Opt-out In Full Model or perhaps the No-consent Model.

Payer Organizations

Payer organizations and the employers that are their client base have a vested interest in efforts to improve healthcare quality and delivery, including engaging individuals in initiatives to improve personal health. Payer organizations also see value in the electronic exchange of health data in terms of potential reductions in their overall expenditures to cover the healthcare costs of enrollees. Thus, payer organizations are similar to provider organizations in preferring "low-resistance" consent models that maximize patient participation and data volume.[36]

HIEs

The individuals responsible for implementing and managing HIEs seek to ensure that the adopted consent policies and procedures (or models) permit the exchanges to fulfill their mission to the community of participants, to evolve over time, and to remain financially viable. HIEs also typically are tasked with building and maintaining the intelligence infrastructure for managing and monitoring consent, including (but not limited to) data capture, application of decision rules for appropriate access, and authentication of eligible providers within the system, such that the individuals responsible for implementing and managing HIEs generally prefer less complicated consent policies and procedures. Such consent procedures also may provide HIEs with more flexibility in terms of allowing participating provider organizations to adopt additional consent procedures, where desired, that exceed the baseline requirements of the HIEs.[37]

[35] Goldstein and Rein 2010a at 27.
[36] Goldstein and Rein 2010a at 27.
[37] Goldstein and Rein 2010a at 28.

D. Consent Models Adopted by Other States

To maximize the benefits of electronic health information, all States have been actively working to establish mechanisms for exchange. Whereas each State HIE makes its determination based on a variety of factors, such as applicable State law, policy, and funding, the issue of patient consent has proven to be a common core challenge for all HIEs. A detailed review of the approved Strategic and Operational Plans and Plan Summaries for all States available from the Federal HHS Office of the National Coordinator for Health Information Technology (ONC) indicates that 3 States have selected a No-consent Model, 27 States have selected an Opt-out Model (either in Full or With Exceptions), and 12 States have selected an Opt-in Model (either In Full or With Restrictions). In addition, 8 States have yet to determine what consent model best suits their needs and interests.

Midwest Examples

For some States, the relevant State laws do not require patient consent for the exchange of health data beyond what is required by Federal law. In **Indiana**, for example, express consent is not required from patients for the electronic exchange of general clinical data for treatment or other State proscribed purposes. Thus, the legal landscape in Indiana has enabled it to adopt a No-consent Model for its exchange (IHIE). However, all participating hospitals in the IHIE must inform patients in their Notice of Privacy Practices that their health data may be used or disclosed for multiple purposes. Further, IHIE requires providers to suppress a patient's health data if the patient requests that his/her information not be shared.[38] Former IHIE President and CEO J. Marc Overhage explained that "IHIE data sources have mutually agreed that certain information [would] not be included in the HIE, like behavioral and mental health."[39] In

[38] AHIMA Conference Issue: http://www.fortherecordmag.com/archives/091310p24.shtml.
[39] AHIMA Conference Issue: http://www.fortherecordmag.com/archives/091310p24.shtml.

addition, programs covered by the Federal Confidentiality of Alcohol and Drug Abuse Patient Records regulations do not provide data to the IHIE.[40] Thus, the types of data typically eligible for exchange in the IHIE include, but are not limited to, medication history, prescription data, immunizations, allergies, laboratory testing results (e.g., pathology and radiology results), electrocardiogram reports, emergency department reports, discharge summaries, and claims processing.[41]

Recently, **Kansas** enacted a new law regarding HIE generally adopting Federal HIPAA rules and policies, and **Wisconsin** has announced a similar intent. **Iowa** also recently enacted a new law regarding HIE generally adopting Federal HIPAA rules and policies, including a broad permission to the exchange of any patient data for purposes of treatment.[42]

The legal landscape and governance structures in other States provide an environment better suited to other consent models. For example, **Kentucky** has selected an Opt-out Model for its electronic exchange (KHIE). Unlike HIPAA regulations, Kentucky regulations governing medical records lack a T-P-O exception. Thus, obtaining patient consent is implemented at the point of care through patient registration materials.[43] KHIE's current sample Notice of Privacy Practices for participants states that KHIE makes patient health data available to other participants who need it for T-P-O purposes. In addition, it states that patients may choose to opt out of having their health data in the KHIE and that "participation is not a condition of receiving

[40] Goldstein and Rein 2010a at 13.
[41] Goldstein and Rein 2010a at 17.
[42] Sec. 14. Section 135.156E, Code 2011.
[43] Governor's Office of Electronic Health Information, *Kentucky Strategic and Operational Plan for Health Information Exchange*, http://chfs.ky.gov/NR/rdonlyres/D0CF5638-DE1C-4468-9AA1-2622F17AAC4F/0/KHIEPl.pdf.

care." Further, KHIE does not store patient health data, but rather, the data are only pulled through the KHIE when participating providers request the patient information.[44]

By contrast, **Missouri** and **Minnesota** are among the minority of States that have adopted an Opt-in approach, most notably including also New York and California.[45] California, concerned with the possibility for "unintended, overly broad, and unnecessary disclosures due to the lack of technological capability to segment data", and aware of the many personal, religious, and cultural reasons that patients might have for not wanting their health data exchanged, California prefers that patients "exercise their right to privacy at the front end."[46] Accordingly, California has selected an Opt-In patient consent model and is developing an educational website for patients and providers to help with making informed consent decisions.[47] Providers may access patient electronic records through the HIE in emergency situations, within set parameters and via a "break the glass" provision, unless the patient has previously withheld or withdrawn his/her consent to electronically exchange his/her health data.[48]

E. Viewing the Core Consent Models as Peaks Within a Continuous Landscape of Options

The five core consent models appear to offer discrete alternatives to incorporating patient choice or input in HIEs. Yet in practice, there are multiple possible permutations of the models.[49] In this sense, the five consent models represent peaks within a continuous landscape of options

[44] KHIE Sample Notice of Privacy Practices for providers, http://khie.ky.gov/nr/Documents/Sample%20Notice%20of%20Privacy%20Practices.pdf
[45] CalOHII Patient Consent and Informing Task Group of the Privacy Steering Team, *Research and Background for Patient Consent Policy Recommendation* (2012).
[46] CalOHII Patient Consent and Informing Task Group of the Privacy Steering Team 2012 at 22-25.
[47] CalOHII Patient Consent and Informing Task Group of the Privacy Steering Team 2012 at 24-28. The Opt-In recommendation will be tested by WHIN (a major Los Angeles HIO) and San Diego Beacon Community. Before making Opt-In the official California policy, the Privacy Steering Committee is meeting to discuss the implications of its recommendations and how to harmonize them with both HIPAA and CMIA. The California Medical Information Act affords patients more privacy than HIPAA alone does.
[48] CalOHII Patient Consent and Informing Task Group of the Privacy Steering Team 2012 at 25.
[49] Goldstein and Rein 2010a at 7.

for HIEs, especially if at least some level of granularity or data segmentation is incorporated. Indeed, some HIEs may have sufficiently flexible policy frameworks to permit multiple permutations of consent models to co-exist.[50] Finding and maintaining the proper balance among the varied and often contrasting needs and interests of the diverse stakeholders in an HIE are likely to be aided significantly by such flexibility, which in turn should help to ensure long-term HIE viability. To varying degrees, flexibility along these lines is evident in each of the three models described above for Indiana, Kentucky, and California.

July 17, 2012 (*revised* July 20, 2012)

[50] Goldstein and Rein 2010a at 7.